

Application No.: 09/632,933
Old Attorney's Docket No. 040070-692
New Attorney's Docket No. 0119-149
Page 5

REMARKS

Claims 1-12 remain pending in the application. It is proposed to amend claims 1 and 6 without introduction of new matter. Entry of these amendments and favorable reconsideration are respectfully requested in view of the above amendments and the following remarks.

Claims 1-10 again stand rejected as allegedly being anticipated by Kruse (US-5,148,007). This rejection is respectfully traversed.

It is well established that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). In the present instance, Kruse fails to anticipate any of claims 1-10 at least because it neither discloses nor suggests any techniques or apparatuses for generating an authentication ciphering offset (ACO) in a communication device. It therefore fails to disclose or suggest any method (independent claim 1) or apparatus (independent claim 6) that includes "generating the ACO as a function of one or more parameters, wherein at least one of the one or more parameters is derived from earlier-computed values of the ACO."

In support of its rejection, the Office alleges that Kruse's authorization parameter (e.g., "AP1") is the equivalent of an ACO, and that the random numbers (e.g., V1) from which the authorization parameter is derived are equivalent to Applicants' at least one of the one or more parameters from which the ACO is generated, which according to Applicants' claims "is derived from earlier-computed values of the ACO."

However, as explained in Applicants' previously-filed response, Kruse's AP1 and AP2 parameters are in no way equivalent to an ACO, nor are Kruse's V1 and V2 parameters used for the purpose of generating an ACO. This is readily seen when one considers that, in systems such as Bluetooth, the creation of an encryption key can be dependant both on a link key and on the ACO. The ACO is a number that is created for every call of the function that generates the SRES (signed response) used for authentication. Consequently, if two units attempt to share data that is encrypted with different ACOs, their respective generated encryption keys will differ from one another, even if the units use the same link key. Importantly, unlike the random number AU RAND, sent by a verifier to a claimant under a challenge-response scheme, and the signed response SRES, sent from the claimant back to

Application No.: 09/632,933
Old Attorney's Docket No. 040070-692
New Attorney's Docket No. 0119-149
Page 6

the verifier, the generated ACOs are not shared between units. Doing otherwise would jeopardize the security of the communication.

In contrast, Kruse's V1 and V2 parameters can correspond to Applicants' AU_RANDOM, and Kruse's AP1 and AP2 parameters can correspond to Applicants' SRES and SRES' described in the application, since Kruse describes that these parameters are used in a challenge-response strategy for authenticating the identity of a party to a communication. In the cited portion relied upon in the Office Action, Kruse describes that that "mutually transmitted, first and second authorization parameters AP1, AP2 are then advantageously used for generating a variable starting value for a new random number". Kruse's Figures 1 and 2 also clearly show that both of these parameters are exchanged between communicating devices. Accordingly, the generation of Kruse's random number requires the mutual exchange of the first and second authorization parameters AP1, AP2 between the devices.

The plain meaning of an ACO, as understood by those of ordinary skill in the art, is a number used for generation of an encryption key that is neither exchanged, nor representative of numbers exchanged, between devices sharing information. Since Kruse's authorization parameters AP1 and AP2 possess neither of these inherent features of claim 1, which recites a method of generating an ACO, the claim is believed not to be anticipated by Kruse as the Office asserts. The same can be said for claim 6, which recites features substantially similar to claim 1.

Applicants believe that the very definition and understanding of an ACO in the art to which Applicants' invention pertains mandates the conclusions expressed above. Nonetheless, in its Response to Arguments, the Office gives no weight to Applicants' arguments because "the features upon which applicant relies ... are not recited in the rejected claims(s)." The Office explains that "[a]lthough the claims are interpreted in light of the specification, limitations from the specification are not read into the claims."

Applicants respectfully disagree that the above arguments require reading limitations from the specification (i.e., about ACOs not being exchanged between devices) into the claims because the features relied on in Applicants' arguments are inherent in every ACO, and were known to those of ordinary skill in the art at the time the application was filed. Thus, no amendment to the claims is believed to be necessary. Nonetheless, in the interest of expediting prosecution of the application, it is now proposed to amend each of independent claims 1 and 6 to further define that "the ACO is a number from which a ciphering key for

Application No.: 09/632,933
Old Attorney's Docket No. 040070-692
New Attorney's Docket No. 0119-149
Page 7

the communication device is derived, and which is never communicated to any other communication device". Since these features were already inherently defined by the claims, it is believed that entry of this amendment would not change the scope of the claims, nor would it require that a new search be performed by the Office.

For at least the foregoing reasons, independent claims 1 and 6, as well as claims 2-5 and 7-10 which variously depend from claims 1 and 6, are believed to be patentably distinguishable over the Kruse patent. Therefore, it is respectfully requested that the above amendments be entered, and that the rejection of claims 1-10 under Section 102 be withdrawn.

Claims 11-12 were rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Kruse as applied to claims 1-10, and further in view of Kunito et al. (US-6,577,633B1). This rejection is respectfully traversed.

Each of claims 11 and 12 depends from claim 6, and is therefore patentable over the Kruse patent for at least the reasons set forth with respect to claim 6. The Kunito et al. patent fails to make up for the deficiencies of Kruse at least because it too, is silent with respect to any techniques or apparatuses for generating an ACO. Therefore, no combination of Kruse with Kunito can disclose Applicants' claimed methods and apparatuses for generating an ACO in a communication device. Accordingly, the Office has failed to make out even a *prima facie* case of obviousness, since one of the necessary criteria for supporting such a rejection is that the prior art references, when combined, must teach or suggest all of the claim limitations. See, e.g., MPEP §2143.


For at least the foregoing reasons, claims 11 and 12 are believed to be patentable over the Kruse and Kunito et al. patents, regardless of whether these documents are considered individually or in combination. It is therefore respectfully requested that the rejection of claims 11-12 under Section 103(a) be withdrawn.

Application No.: 09/632,933
Old Attorney's Docket No. 040070-692
New Attorney's Docket No. 0119-149
Page 8

The application is believed to be in condition for allowance. Entry of the above amendments and prompt notice of allowance are respectfully requested.

Respectfully submitted,
Potomac Patent Group PLLC

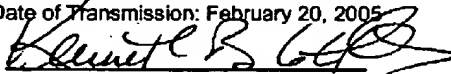
Date: February 20, 2005

By: 
Kenneth B. Leffler
Registration No. 36,075

P.O. Box 855
McLean, Virginia 22101-0855
703-718-8884

I hereby certify that this correspondence is being sent by facsimile transmission to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 to the following facsimile number:

Facsimile Number: 703 872 9306
Date of Transmission: February 20, 2005


Kenneth B. Leffler